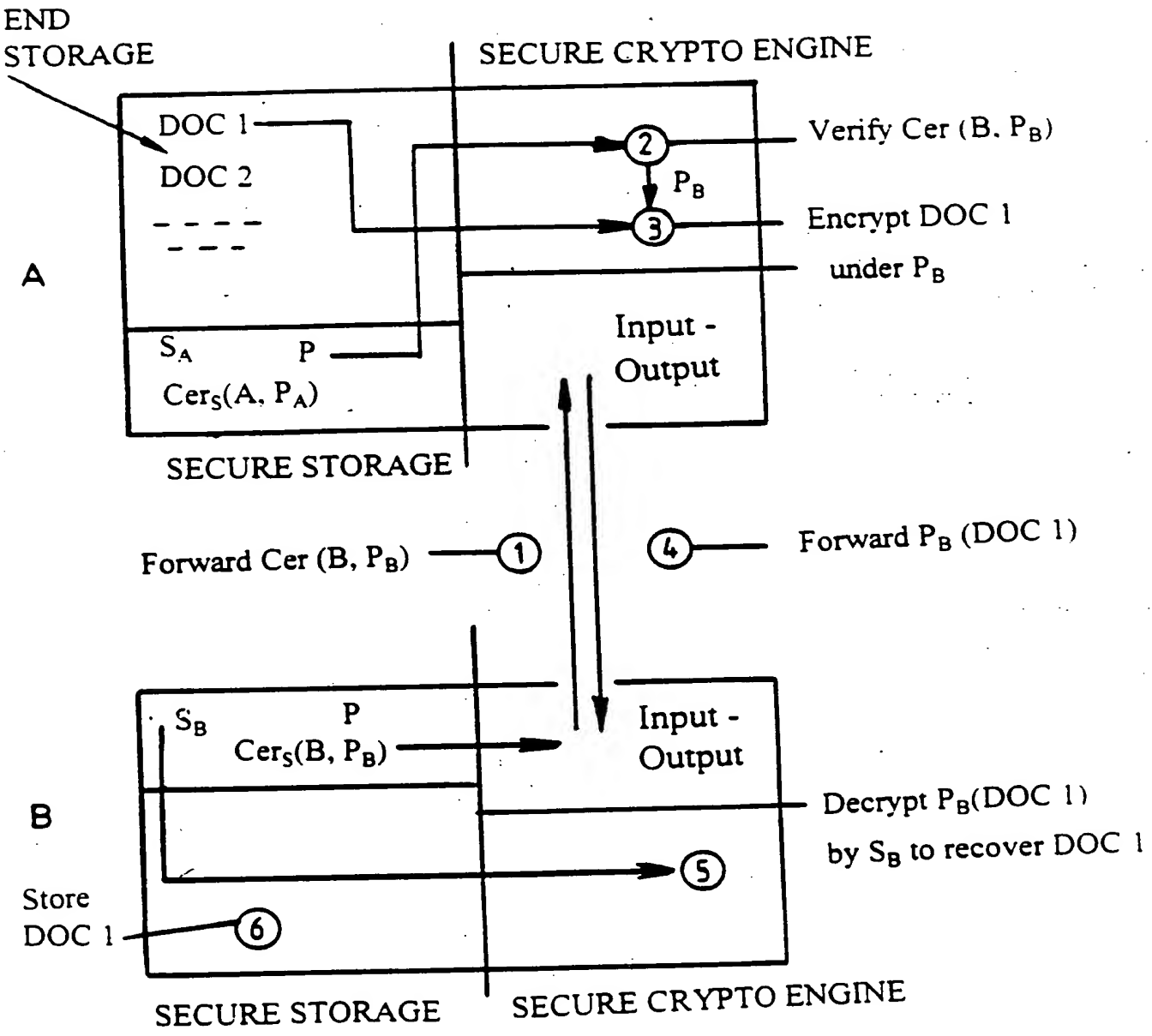
FIG. 1



P: Public key of CA

S: Secret key of CA

FIG.2

END Generation

CREATE CONTENT	END
⇓	
ADD TIMESTAMP	END + T ---> STORE
⇓	
CALCULATE HASH	$h(END + T) = h_1$
⇓	
	END OUTSIDE
INPUT D-C	{
	h_1 INSIDE
⇓	
APPEND DEVICE NO.	D(j)
⇓	
APPEND SEQ. NO.	S(i)
⇓	
(APPEND WM = IDENTIFICATION)	
⇓	
CALCULATE HASH	$h(h_1 + D(j) + S(i) + WM) = h_2$
⇓	
SIGN HASH	$S_j(h_2)$
⇓	
STORE	$h(h_1 + D(j) + S(i) + WM), S_j(h_2)$
⇓	
APPEND COUNTER = "0", FLAG = "1" (SELL)	

FIG.3

NEGOTIATION

Stage	SELLER, using D-C_A		BUYER, using D-C_B
1		<---	Send public key P_B cert. C_B
2	Verify Certificate C_B	by D-C_A	
3	Specify D(j), S(i)	input	
4	Verify flag = 1	by D-C_A	
5	Encrypt specified END record M under P_B to generate ciphertext C		
6	Set flag = 0, send C, END and certificate of Issuer (j)	--->	
7		by D-C_B	Decrypt C
8		by D-C_B	Verify issuer's signature
9		by owner	Check validity period
10			Store in new END record
11			Increment counter, set flag = 1